COPY

AO 106 (Rev. 04/10) Application for a Search Warrant (USAO CDCA Rev. 01/2013)

UNITED STATES DISTRICT COURT

for the

Central District of California

FILED
CLERK, U.S. DISTRICT COURT
SEP - 8 2015
CENTRAL DISTRICT OF CALIFORNIA
BY DEPUTY

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)
a 2013 Chrysler 200, assigned VIN 1C3CCBBB5DN763255 and CA License Plate Number 7HLM273

Case No. 15-1670M

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

See Attachment A

located in the Central District of California, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

☑ evidence of a crime;
☑ contraband, fruits of crime, or other items illegally possessed;
☑ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
21 U.S.C. Secs. 846 and 841(a)(1) - conspiracy to dist. cocaine	See attached Affidavit

The application is based on these facts:
See attached Affidavit

☑ Continued on the attached sheet.
☐ Delayed notice of _____ days (give exact ending date if more than 30 days: ___________) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

/s/
Applicant's signature

William Cone III, Special Agent, FBI
Printed name and title

Sworn to before me and signed in my presence.

Date: 9-8-15

Suzanne H. Segal
Judge's signature

City and state: Los Angeles, California

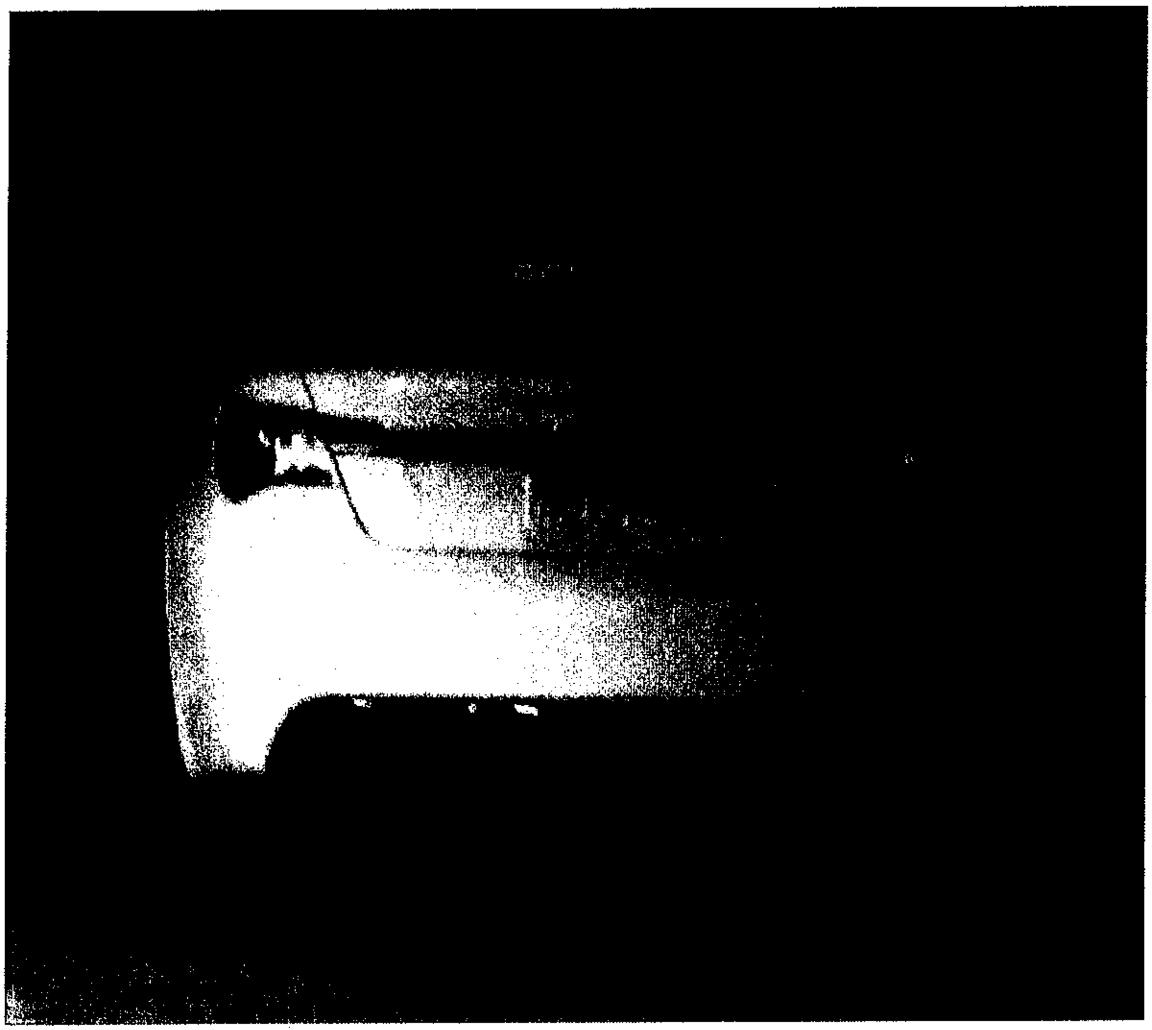
Hon. Suzanne H. Segal, U.S. Magistrate Judge
Printed name and title

AUSA: Joanna Curtis x10298

Attachment A

White Chrysler 200, VIN# 1C3CCBBB5DN763255 bearing CA license plate "7HLM273"

The White Chrysler 200 vehicle, bearing California License Plate "7HLM273," with a yellow section above the rear license plate. The Chrysler has four doors, four rubber tires, two side mirrors, with clear non-tinted windows and sometimes has a removable blue handicapped parking tag hanging in the interior of the vehicle. VIN 1C3CCBBB5DN763255 is on a silver plate affixed to Target Location #2's dashboard and is visible on the bottom of the driver's side front windshield.



ATTACHMENT B

I. ITEMS TO BE SEIZED

1. The items to be seized are evidence, fruits, and instrumentalities of violations of Title 21, United States Code, Sections 846 and 841, that is, conspiracy to distribute five kilograms or more of cocaine, namely:

a. Records, documents, programs, applications, or materials relating to or memorializing the facilitation of distribution of controlled substances, including any currency in amounts exceeding $1,000, buyers lists, seller lists, pay/owe sheets, records of sales, log books, drug ledgers, telephone answering pads, bank and financial records, storage records such as storage locker receipts, and safe deposit box rental records;

b. Records, documents, programs, applications, or materials and articles of personal property relating to the identity of persons occupying, possessing, residing in, owning, frequenting or controlling the premises to be searched or property therein, including keys, rental agreements and records, property acquisition records, utility and telephone bills and receipts, photographs, answering machine tape recordings, telephone beeper or paging devices, rolodexes, telephone/communication devices answering pads, storage records, vehicle and/or vessel records, canceled mail envelopes, correspondence, financial documents such as tax returns, bank records, safe deposit records, canceled checks, and other records of income and expenditure, credit card and bank records, travel documents, personal identification documents, and documents

relating to obtaining false identification, including birth certificates, driver's license, immigration cards and other forms of identification in which the same person would use other names and identities other his/her own;

c. Chemicals and/or equipment used for manufacturing, packaging, weighing, cutting, testing, distributing and identifying controlled substances;

d. Records, documents, programs, applications, or materials and articles of personal property relating to the commission of a conspiracy to conduct narcotics trafficking, including precious metals, jewelry, written correspondence, video tape recordings, photographs and/or drawings related to narcotics trafficking activities.

e. Any digital device used to facilitate the above-listed violations and forensic copies thereof.

f. With respect to any digital device used to facilitate the above-listed violations or containing evidence falling within the scope of the foregoing categories of items to be seized:

i. evidence of who used, owned, or controlled the device at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, e-mail, e-mail contacts, chat and instant messaging logs, photographs, and correspondence;

ii. evidence of the presence or absence of software that would allow others to control the device, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence

of the presence or absence of security software designed to detect malicious software;

iii. evidence of the attachment of other devices;

iv. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the device;

v. evidence of the times the device was used;

vi. passwords, encryption keys, and other access devices that may be necessary to access the device;

vii. applications, utility programs, compilers, interpreters, or other software, as well as documentation and manuals, that may be necessary to access the device or to conduct a forensic examination of it;

viii. records of or information about Internet Protocol addresses used by the device;

ix. records of or information about the device's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

2. As used herein, the terms "records," "documents," "programs," "applications," and "materials" include records, documents, programs, applications, and materials created, modified, or stored in any form, including in digital form on any digital device and any forensic copies thereof.

3. As used herein, the term "digital device" includes any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop,

laptop, notebook, and tablet computers; personal digital assistants; wireless communication devices, such as telephone paging devices, beepers, mobile telephones, and smart phones; digital cameras; peripheral input/output devices, such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices, such as modems, routers, cables, and connections; storage media, such as hard disk drives, floppy disks, memory cards, optical disks, and magnetic tapes used to store digital data (excluding analog tapes such as VHS); and security devices.

II. SEARCH PROCEDURE FOR DIGITAL DEVICES

4. In searching digital devices or forensic copies thereof, law enforcement personnel executing this search warrant will employ the following procedure:

a. Law enforcement personnel or other individuals assisting law enforcement personnel (the "search team") will, in their discretion, either search the digital device(s) on-site or seize and transport the device(s) to an appropriate law enforcement laboratory or similar facility to be searched at that location. The search team shall complete the search as soon as is practicable but not to exceed 60 days from the date of execution of the warrant. If additional time is needed, the government may seek an extension of this time period from the Court on or before the date by which the search was to have been completed.

b. The search team will conduct the search only by using search protocols specifically chosen to identify only the specific items to be seized under this warrant.

i. The search team may subject all of the data contained in each digital device capable of containing any of the items to be seized to the search protocols to determine whether the device and any data thereon falls within the list of items to be seized. The search team may also search for and attempt to recover deleted, "hidden," or encrypted data to determine, pursuant to the search protocols, whether the data falls within the list of items to be seized.

ii. The search team may use tools to exclude normal operating system files and standard third-party software that do not need to be searched.

c. When searching a digital device pursuant to the specific search protocols selected, the search team shall make and retain notes regarding how the search was conducted pursuant to the selected protocols.

d. If the search team, while searching a digital device, encounters immediately apparent contraband or other evidence of a crime outside the scope of the items to be seized, the team shall immediately discontinue its search of that device pending further order of the Court and shall make and retain notes detailing how the contraband or other evidence of a crime was encountered, including how it was immediately apparent contraband or evidence of a crime.

e. If the search determines that a digital device does not contain any data falling within the list of items to be seized, the government will, as soon as is practicable, return the device and delete or destroy all forensic copies thereof.

f. If the search determines that a digital device does contain data falling within the list of items to be seized, the government may make and retain copies of such data, and may access such data at any time.

g. If the search determines that a digital device is (1) itself an item to be seized and/or (2) contains data falling within the list of items to be seized, the government may retain forensic copies of the digital device but may not access them (after the time for searching the device has expired) absent further court order.

h. The government may retain a digital device itself until further order of the Court or one year after the conclusion of the criminal investigation or case (whichever is latest), only if the device is determined to be an instrumentality of an offense under investigation or the government, within 14 days following the time period authorized by the Court for completing the search, obtains an order from the Court authorizing retention of the device (or while an application for such an order is pending). Otherwise, the government must return the device.

i. Notwithstanding the above, after the completion of the search of the digital devices, the government shall not access digital data falling outside the scope of the items to be seized absent further order of the Court.

5. In order to search for data capable of being read or interpreted by a digital device, law enforcement personnel are authorized to seize the following items:

a. Any digital device capable of being used to commit, further or store evidence of the offenses listed above;

b. Any equipment used to facilitate the transmission, creation, display, encoding, or storage of digital data;

c. Any magnetic, electronic, or optical storage device capable of storing digital data;

d. Any documentation, operating logs, or reference manuals regarding the operation of the digital device or software used in the digital device;

e. Any applications, utility programs, compilers, interpreters, or other software used to facilitate direct or indirect communication with the digital device;

f. Any physical keys, encryption devices, dongles, or similar physical items that are necessary to gain access to the digital device or data stored on the digital device; and

g. Any passwords, password files, test keys, encryption codes, or other information necessary to access the digital device or data stored on the digital device.

6. The special procedures relating to digital devices found in this warrant govern only the search of digital devices pursuant to the authority conferred by this warrant and do not apply to any search of digital devices pursuant to any other court order.

AFFIDAVIT

I, William Cone III, being duly sworn, declare and state as follows:

I. INTRODUCTION

1. I am a Special Agent ("SA") with the United States Federal Bureau of Investigation ("FBI"), and have been so employed for approximately five years. After completing my training at the FBI Academy located in Quantico, Virginia, I was assigned to the Santa Ana Resident Agency of the FBI's Los Angeles Field Office ("LAFO"), where I worked on a counterterrorism squad investigating state-sponsored terrorist groups. Since July 2013, I have been assigned to LAFO's Transnational Organized Crime - Eastern Hemisphere Squad, where I investigate violations of federal law related to violent and organized crime, art theft, access device fraud, and bank fraud.

2. This affidavit is made in support of applications for search warrants for the following:

a. 5416 North Fair Avenue, Apartment 6-104, North Hollywood, California 91601 (hereinafter referred to as "**Target Location #1**");

b. a 2013 Chrysler 200, assigned VIN 1C3CCBBB5DN763255 and California License Plate Number 7HLM273 (hereinafter referred to as "**Target Location #2**");

c. 7950 West Sunset Boulevard, Apartment 514, Los Angeles, California 90046 (hereinafter referred to as "**Target Location #3**");

d. a 2011 Porsche Panamera, assigned VIN WP0AA2A72BL019885 and personalized California License Plate Number "3 TEN CO" (hereinafter referred to as "**Target Location #4**");

e. safe deposit box #312, which is located and maintained at the business identified as US Private Vaults, 9182 West Olympic Boulevard, Beverly Hills, California 90212 (hereinafter referred to as "**Target Location #5**");

f. safe deposit box #4102, which is located and maintained at the business identified as US Private Vaults, 9182 West Olympic Boulevard, Beverly Hills, California 90212 (hereinafter referred to as "**Target Location #6**"); and

g. safe deposit box #4404, which is located and maintained at the business identified as US Private Vaults, 9182 West Olympic Boulevard, Beverly Hills, California 90212 (hereinafter referred to as "**Target Location #7**")

to seize evidence, fruits, and instrumentalities, as specified in Attachment B, which is also attached hereto and incorporated by reference, of violations of Title 21, United States Code, Sections 846 and 841(a)(1), that is, conspiracy to distribute 5 kilograms or more of cocaine (hereinafter referred to as the "**Target Offenses**").

3. The facts set forth in this affidavit are based upon conversations I have had with other law enforcement officers, a review of reports and written summaries generated by other law enforcement officers, and my training and experience. This affidavit is being submitted for the limited purpose of

establishing probable cause for the issuance of the requested search warrants. As such, this affidavit does not contain all of the facts and circumstances that I have learned during this investigation. Unless specifically indicated otherwise, all conversations and statements described in this affidavit are related in substance and in part only.

II. PREMISES TO BE SEARCHED

4. The search locations are described as follows and in Attachment A, which is attached hereto and incorporated herein by reference:

a. **Target Location #1** is 5416 North Fair Avenue, Apartment 6-104, North Hollywood, California 91601. 5416 North Fair Avenue is a multi-unit apartment complex which is located on the east side of Fair Avenue, south of Cumpston Street, and North of Chandler Boulevard, and which appears to be of wood frame construction. It has an off-white, brown, and green stucco exterior, windows with black metal trim, and a low-slope (flat) roof. The address "5416 North Fair Avenue" is displayed across the front of the structure. On the map of the complex, Apartment 6-104 is located in the building labeled "6" which is east of Fair Avenue, in the central part of the complex. The door to Apartment 6-104 is dark brown in color, with a silver-covered bolt lock above a silver-colored handle on the left side of the door. The door also has a "peep-hole" in the center of the door slightly under the top of the door. To the left of the

door is a square with "6-104" and five dots underneath the numbers.

b. **Target Location #2** is a White Chrysler 200 vehicle, bearing California License Plate "7HLM273," with a yellow section above the rear license plate. Target Location #2 has four doors, four rubber tires, two side mirrors, with clear non-tinted windows and sometimes has a removable blue handicapped parking tag hanging in the interior of the vehicle. VIN 1C3CCBBB5DN763255 is on a silver plate affixed to Target Location #2's dashboard and is visible on the bottom of the driver's side front windshield.

c. **Target Location #3** is 7950 West Sunset Boulevard, Apartment 514, Los Angeles, California 90046. Target Location #3 is located south of West Sunset Boulevard and west of Hayworth Avenue. 7950 West Sunset Boulevard is a multi-unit apartment complex which appears to be of wood frame construction. Target Location #3 has an off-white, brown, and yellow stucco exterior, windows with white/gray metal trim, and a low-slope (flat) roof. The address "7950 West Sunset" is displayed along the north side of the structure. Apartment 514 is on the fifth floor of the building. The door to Apartment 514 is dark brown in color, with two silver-covered bolt locks above a silver-colored handle on the left side of the door. The door also has a "peep-hole" in the center of the door slightly under the top of the door. To the left of the door is a square with "514" displayed in black over a gray-colored placard.

d. **Target Location #4** is a matte black Porsche Panamera vehicle, bearing California License Plate "3 TEN CO" mounted in a burgundy, black, and gold color license plate holder that has "Alumni" displayed across the top and "USC" displayed across the bottom. **Target Location #4** has four doors, four rubber tires, two side mirrors, and tinted dark windows. VIN WP0AA2A72BL019885 is on a silver plate affixed to Target Location #4's dashboard and is visible on the bottom of the driver's side front windshield.

e. **Target Location #5** is a safety deposit box, bearing number 312, located at U.S. Private Vaults, 9182 West Olympic Boulevard, Beverly Hills, California 90212. U.S. Private Vaults is a storefront vault business. The storefront is located in a strip mall-type structure on the south side of West Olympic Boulevard, west of South Oakhurst Drive, and east of South Palm Drive. The storefront has glass front windows with a lighted sign above the front door that reads "US Private Vaults" in blue and red colors. The front door to the storefront faces north toward West Olympic Boulevard and has the address "9182" displayed on the front door. Safe deposit box number 312 is located inside the business and is constructed of a metal type of material, has a shiny metallic color, has a key lock on the front, and has the box number "312" displayed on the front of the box.

f. **Target Location #6** is a safety deposit box, bearing box number 4102, located at U.S. Private Vaults, 9182 West Olympic Boulevard, Beverly Hills, California 90212. U.S.

Private Vaults is a storefront vault business. The storefront is located in a strip mall-type structure on the south side of West Olympic Boulevard, west of South Oakhurst Drive, and east of South Palm Drive. The storefront has glass front windows with a lighted sign above the front door that reads "US Private Vaults" in blue and red colors. The front door to the storefront faces north toward West Olympic Boulevard and has the address "9182" displayed on the front door. Safe deposit box number 4102 is located inside the business and is constructed of a metal type of material, has a shiny metallic color, has a key lock on the front, and has the box number "4102" displayed on the front of the box.

g. **Target Location #7** is a safe deposit box, bearing box number 4404, located at U.S. Private Vaults, 9182 West Olympic Boulevard, Beverly Hills, California 90212. U.S. Private Vaults is a storefront vault business. The storefront is located in a strip mall-type structure on the south side of West Olympic Boulevard, west of South Oakhurst Drive, and east of South Palm Drive. The storefront has glass front windows with a lighted sign above the front door that reads "US Private Vaults" in blue and red colors. The front door to the storefront faces north toward West Olympic Boulevard and has the address "9182" displayed on the front door. Safe deposit box number 4404 is located inside the business and is constructed of a metal type of material, has a shiny metallic color, has a key lock on the front, and has the box number "4404" displayed on the front of the box.

III. SUMMARY OF PROBABLE CAUSE

5. After several in-person meetings between an undercover FBI agent ("UC") and Owen Hanson ("Hanson"), the UC and Hanson exchanged a series of encrypted email messages between July 18, 2015, and August 5, 2015. During the exchange of those encrypted email messages, Hanson arranged to "front" the UC two kilograms of cocaine and to sell the UC an additional three kilograms of cocaine at a price of $30,000 per kilogram. Hanson lives at **Target Location #3** and owns **Target Location #4.** Additionally, Hanson is the lessee of the safe deposit boxes designated as **Target Location #5**, **Target Location #6**, and **Target Location #7**. In a recent meeting and during his ongoing exchange of encrypted emails with the UC, Hanson stated that he has used his safe deposit box at U.S. Private Vaults to store proceeds of illegal activity.

6. Consistent with the arrangement that Hanson made with the UC during their exchange of encrypted emails, five kilograms of cocaine were delivered to the UC's "employees" (who were actually other undercover law enforcement officers) at a hotel in San Diego, California, on August 5, 2015. The delivery was made by Rufus Leon Rhone, aka Junior ("Rhone"), who lives at **Target Location #1** and who used **Target Location #2** to transport the cocaine to the delivery location and to transport the $90,000 in drug proceeds from the transaction site in San Diego to **Target Location #1** in Los Angeles.

IV. STATEMENT OF PROBABLE CAUSE

A. Hanson's Cocaine Distribution And Money Laundering Activities in Australia

7. I have spoken with the agents involved in this investigation, and read their written reports, and have learned the following:

a. The FBI became aware of Hanson during a previous investigation conducted by the FBI's San Diego Field Office ("SDFO") which reached the indictment phase in 2013. As Hanson was not the focus of that investigation, he was not included in those indictments. Following those indictments, SDFO began an investigation into Hanson's suspected criminal activities.

b. On July 11, 2015, the UC conducted a recorded meeting with Hanson. During the meeting, which took place in San Diego, Hanson told the UC that he was involved in distributing cocaine in Australia. Hanson stated that he was getting "kilos" of high quality cocaine from Mexican suppliers and that he delivered the cocaine to his distributors in Australia, who sold the cocaine for a large profit. Hanson further stated that cocaine is like "gold" or "precious metal" in Australia, and that his associates sell it for $175,000 per kilogram. Hanson stated that he had made a significant amount of money selling cocaine in Australia and asked if the UC could transport his drug proceeds from Australia to the United States. The UC agreed to "move" (i.e., launder) Hanson's drug money from Australia to the United States for an 8% commission fee. Hanson informed the UC that he only uses "PGP" (a commonly-used acronym to describe the message

encryption technology program "pretty good privacy") to communicate with his "associates" and "runners" (individuals involved in the distribution of cocaine and the movement of drug proceeds). Surveillance agents observed Hanson depart the meeting in **Target Location #4.**

c. On July 18, 2015, the UC conducted another recorded meeting with Hanson. During the meeting, which occurred in San Diego, Hanson arranged to have one of his "runners" in Australia deliver $100,000 in drug proceeds to the UC's "employee" (who was in fact an undercover Australian law enforcement officer), so that the UC could have the money transported to the United States.

d. On July 21, 2015, pursuant to these negotiations between the UC and Hanson, a "runner" working for Hanson delivered $200,050 Australian dollars (the equivalent of approximately $144,335 in U.S. currency) to a person whom Hanson and his runner believed to be a runner working for the UC, but who was in fact an undercover police officer in Sydney, Australia. At the direction of Hanson, the UC wire transferred that money as follows: $50,000 into a Bank of America bank account in the name of "Hanson Builders"; $50,000 into a JP Morgan Chase Bank account in the name of "Inmobilaria Rolling Hills SA"; and $32,750 in cash to a "runner" employed by Hanson. The remaining $11,550 was kept by the UC pursuant to the 8% money laundering commission fee to which Hanson had previously agreed.

e. A second money laundering delivery took place in Sydney, Australia, on July 27, 2015. On that day, a "runner" working for Hanson delivered $250,000 Australian dollars (the equivalent of approximately $179,527 in U.S. currency) to a person whom Hanson and his runner believed to be a runner working for the UC, but who was in fact an undercover police officer in Sydney, Australia. At the direction of Hanson, the UC wire transferred that money as follows: $120,000 into a JP Morgan Chase Bank account in the name of "Inmobilaria Rolling Hills SA"; and $45,000 in cash to a "runner" employed by Hanson. The remaining $14,500 was kept by the UC pursuant to the 8% money laundering commission fee to which Hanson had previously agreed.

B. Five Kilogram Cocaine Delivery

8. I have spoken with the agents involved in this investigation, and read their written reports, and have learned the following:

a. On August 5, 2015, Rhone delivered five kilograms of cocaine to undercover law enforcement officers at a location in San Diego, California. Rhone made that delivery on behalf of his employer, Hanson. Agents conducting surveillance of the five-kilogram cocaine delivery confirmed that Rhone used **Target Location #2** to transport and deliver the cocaine, and that he used **Target Location #2** to transport the proceeds of the cocaine sale ($90,000) from San Diego to Los Angeles. The details of that transaction are as follows.

b. On July 18, 2015, in addition to discussing the manner in which the UC would, at Hanson's direction, launder Hanson's drug proceeds in Australia, the UC and Hanson also discussed conducting the sale of cocaine. The UC and Hanson also discussed a cocaine sale in subsequent PGP encrypted messages. Hanson agreed to "front" (sell on consignment) the UC two kilograms of cocaine and to sell an additional three kilograms of cocaine to the UC at a price of $30,000 per kilogram.

c. In a series of PGP encrypted messages from July 18, 2015, to August 5, 2015, Hanson and the UC confirmed the details of the five-kilogram cocaine delivery. Hanson stated that he would send a black male, to whom he referred as "Junior," to make the cocaine delivery. Hanson and the UC agreed that the delivery would take place at a hotel in Del Mar, California.

d. Consistent with the arrangement Hanson had made with the UC, on August 5, 2015, a black male, who as set forth below was subsequently identified as Rhone, arrived at the prearranged hotel in Del Mar, California. Upon arriving at that location, Rhone gave an undercover law enforcement officer (who was posing as the UC's employee) one kilogram of cocaine. Rhone stated that he lived in the Hollywood area of Los Angeles (the area in which **Target Location #1** is located), and that he was a "driver" for his "boss." Upon testing a sample taken from the kilogram and confirming that it was cocaine, the undercover officer agreed to exchange $90,000 for the remaining kilograms of cocaine. Rhone stated that the additional four kilograms of cocaine were in a box in his car (**Target Location #2**).

Surveillance officers observed Rhone walk out of the hotel to **Target Location #2**, and drive **Target Location #2** to the front of the hotel where an undercover officer retrieved the additional four kilograms from the front seat of **Target Location #2**, while another undercover officer gave Rhone a bag containing $90,000.

e. Surveillance officers observed Rhone place the bag containing that money in **Target Location #2** and then drive to **Target Location #1.** Rhone made two brief stops during the drive between Del Mar and **Target Location #1** – a fast food restaurant and a post office. Surveillance officers did not observe Rhone bring the bag containing the $90,000 into either of those locations.

f. In a series of PGP encrypted messages with Hanson, the UC confirmed that the five-kilogram cocaine delivery had occurred as planned. In fact, the cocaine had been secured in an evidence room at FBI.

g. On August 25, 2015, the UC informed Hanson that the two kilograms of cocaine Hanson had "fronted" the UC had been successfully smuggled into Australia. Hanson expressed relief that the cocaine had made it to Australia undetected, stating that he had been "over here stressing for [the] last 3 days," worrying about the delivery.

C. Miami Meeting

9. I have spoken with the agents involved in this investigation, and they informed me of the following:

a. On September 2, 2015, in Miami, Florida, Hanson met with the UC and offered to provide the UC with five kilograms of

ice methamphetamine. Hanson offered to "front" the UC with three of the kilograms of ice methamphetamine, with the intention that they be smuggled into Australia on Hanson's behalf. The UC would purchase the remaining two kilograms of ice methamphetamine for a price to be negotiated later. Hanson indicated he would have the same runner, "Junior," deliver the ice methamphetamine to the UC's employees in San Diego. Hanson told the UC that he had ordered the five kilograms and would attempt to have them delivered sometime early during the week of September 7, 2015.

D. There is Probable Cause to Believe that Evidence Will Be Found at The Target Locations.

10. For each of the Target Locations identified in this affidavit, there is probable cause to believe that evidence, fruits, and instrumentalities of criminal conduct will be found, as set forth below.

a. **Target Location #1.** As noted above, on August ~~7~~, 5 WHC 2015, agents followed Rhone from the location of the five-kilogram cocaine delivery back to **Target Location #1.** Thereafter, on August 18, 2015, agents conducted surveillance of Rhone. After observing Rhone drive **Target Location #2** into the parking lot of **Target Location #1,** agents then observed Rhone gain access to **Target Location #1** using a set of keys.

b. Agents caused a search to be conducted for the registered owner of **Target Location #2,** Sophia L.McReynolds, in the CLEAR online database, a database which contains current and historical proprietary and public records. The results of the

search in the CLEAR database listed "Rufus Leon Rhone, Jr." as an "associate." Further checks within the Accurint online database, which also contains current historical proprietary and public records, for Rhone revealed that Rhone had been listed in proprietary and public records at **Target Location #1** from 2008-2010.

c. The birth date and Social Security number in the CLEAR system for Rufus Leon Rhone Jr. was June 5, 1981, and XXX-XX-5186. Agents queried the California DMV database for Rufus Leon Rhone Jr. and determined that a person named Rufus Leon Rhone Jr. has a California driver's license number of xxxx1659, and a date of birth of June 5, 1981. The DMV address listed for Rufus Leon Rhone Jr. was 11220 Moorepark #123, Studio City, California 91604. Special Agents who had observed the person who delivered five kilograms of cocaine to the UC on August 5, 2015, as set forth above, reviewed the photograph of Rufus Leon Rhone Jr., from the California DMV and confirmed that the person depicted in the California DMV photograph of Rufus Leon Rhone, Jr., date of birth June 5, 1981, and California driver's license number xxxx1659, was in fact the same person. In this way, FBI was able to identify Rhone as one of Hanson's "runners."

d. **Target Location #2.** As set forth above, agents have observed Rhone driving **Target Location #2** on several occasions. Moreover, Rhone used **Target Location #2** to deliver five kilograms of cocaine and transport $90,000 in drug proceeds on August 5, 2015. A DMV records check for **Target Location #2** indicates that it is registered to Sophia L. McReynolds at

Target Location #1. I have spoken with the agents involved in this investigation, and they believe that McReynolds is Rhone's live-in girlfriend or cohabitant. In addition to both McReynolds and Rhone having the same address listed in the CLEAR database, I also know from my training and experience that it is not unusual for individuals involved in drug trafficking activities to register vehicles in the names of their girlfriends, friends, or relatives to (1) conceal the true ownership of the vehicles in order to avoid drug-related forfeiture laws and (2) to frustrate law enforcement efforts to identify the true users of the vehicles through registration checks.

e. **Target Location #3.** Target Location #3 is Hanson's residence. On August 25, 2015, an administrative subpoena was served on the management company of the apartment building in which **Target Location #3** is located. I have been informed that the management company informed agents that Hanson (along with his father, James Hanson) is the lessee of **Target Location #3.** The management company also confirmed that Hanson has a Porsche Panamera (**Target Location #4)** registered to him at this complex for parking purposes.

f. **Target Location #4.** California DMV records demonstrate that Hanson is the registered owner of **Target Location #4.** Law enforcement officers observed Hanson drive **Target Location #4** to and from the above-noted meetings with the UC, and Hanson has informed the UC that he owns **Target Location #4.**

g. **Target Locations #5, #6 and #7.** Target Locations #5, #6, and #7 are safe deposit boxes rented by Hanson. I have spoken with the agents involved in the investigation, and learned that in August and September 2015, during recorded meetings with the UC and in a subsequent PGP encrypted message, Hanson stated that he stored drug and criminal proceeds in an unspecified safety deposit box at "U.S. Private Vaults." Hanson also stated that the owner of the business is Mark Paul, a friend of his. In fact, Hanson told the UC that Paul would give the UC a 40% discount on the rental of a safe deposit box if the UC told Paul he was referred to the business by "Mr. O." During a conversation with the UC on August 21, 2015, Hanson stated that he had an unspecified amount of "gold bullion" stored at "U.S. Private Vaults." In a PGP encrypted message to the UC on August 22, 2015, Hanson stated that at one time he had "over a cost of ferrari" stored at U.S. Private Vaults and that the UC could "keep whatever u want [in a rented safe deposit box], they [the police] arnt coming in there."

h. Agents have confirmed that the owner of U.S. Private Vaults, the location of **Target Locations #5, #6, and #7**, is in fact Mark Paul, the owner previously identified by Hanson. In addition, video footage obtained from U.S. Private Vaults in December 2013 depicts an individual who appears to be Hanson accessing a safe deposit box that cannot be identified on the video. The video footage identified the retina scan associated with Hanson. In August 2015, agents issued an administrative subpoena to U.S. Private Vaults, based on the information

associated with the video footage and retina scan,and confirmed that **Target Locations #5, #6, and #7** were originally rented by a single individual in June 2012 and that the rent on those boxes has been paid through June of 2016.

i. I have spoken with the agents involved, and they believe that Hanson's use of **Target Locations #5, #6, and #7** to store the proceeds from his illegal activities is based in part on the fact that U.S. Private Vaults has a lenient identification and security protocol for its renters. U.S. Private Vaults does not require renters to produce any form of identification to obtain a safe deposit box. Rather, rent on the boxes is paid in cash and access to the facility is via retina scan - the only personally identifiable information kept on file by the business. Once a renter gains access to facility via retina scan, he/she then accesses his/her safety deposit box using a key specific to the rented box. Because there is a limited paper trail generated by the renting of boxes at U.S. Private Vaults, the agents involved believe it is ideal for the concealing and storage of illicit proceeds.

V. TRAINING AND EXPERIENCE - DRUG CASES

11. Based upon my training and experience as a Special Agent, and consultations with law enforcement officers experienced in narcotics, money laundering, financial, racketeering, and all the facts and opinions set forth in this affidavit, I know the following:

a. Individuals involved in narcotics trafficking and money laundering from narcotics trafficking often maintain

documentation evidencing such criminal activity at their residences and in their own vehicles, as well as in the residences and vehicles of their associates, places of business, and/or rental storage locations in order to keep track of the ordering, purchasing, storage, distribution, and transportation of narcotics. At times, the narcotics may be sold, but documentary records and ledgers often remain for long periods of time to memorialize past transactions, the status of accounts receivable and accounts payable, and the names and contact information of suppliers, customers, and co-conspirators. These records are not only maintained in paper form, but also on computer data in the form of computer hardware and software, telephonic devices, and other communication devices.

b. Individuals involved in narcotics trafficking and money laundering from narcotics trafficking will often maintain documentation evidencing such criminal activity at their residences and vehicles, as well as in the residences and vehicles of their associates, place of business, and/or rental storage for long periods of time to memorialize past transactions, client lists, pay/owe sheets and ledgers, runner logs, transaction logs, names and contacts of co-conspirators, the status of accounts receivable and accounts payable. These records are not only maintained in paper form, but also as computer data in the form of computer hardware and software, telephonic devices, and other communication devices.

c. Individuals involved in narcotics trafficking [and money laundering necessitated by the large volume of cash

generated by drug trafficking] often use cellular telephones and PGP-encrypted devices to direct the narcotics trafficking and money laundering with co-conspirators, and to direct or be directed involving all activities associated with their schemes.

d. The above-described documents are often permanently possessed by drug dealers/manufacturers much the same way a legitimate business maintains records and tools of its trade whether or not the business has a particular item in inventory on a given date. These documents are kept by drug dealers/manufacturers whether or not the dealer/manufacturer is in possession of any drugs/chemicals at any given moment. I believe that the seizure of such documents will provide evidence of the events set forth in this affidavit and that such documents can be found in the **Target Locations** despite any lapse of time between the events described and the anticipated search pursuant to this warrant.

e. Additionally, individuals engaged in high cash volume activities, including narcotics trafficking, often times convert cash to other things, including precious metals and jewelry.

VI. TRAINING AND EXPERINCE ON DIGITAL DEVICES

12. As used herein, the term "digital device" includes any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop, laptop, notebook, and tablet computers; personal digital assistants; wireless communication devices, such as telephone paging devices, beepers, mobile telephones, and smart

phones; digital cameras; peripheral input/output devices, such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices, such as modems, routers, cables, and connections; storage media, such as hard disk drives, floppy disks, memory cards, optical disks, and magnetic tapes used to store digital data (excluding analog tapes such as VHS); and security devices. Based on my knowledge, training, and experience, as well as information related to me by agents and others involved in the forensic examination of digital devices, I know that data in digital form can be stored on a variety of digital devices and that during the search of a premises it is not always possible to search digital devices for digital data for a number of reasons, including the following:

a. Searching digital devices can be a highly technical process that requires specific expertise and specialized equipment. There are so many types of digital devices and software programs in use today that it is impossible to bring to the search site all of the necessary technical manuals and specialized equipment necessary to conduct a thorough search. In addition, it may be necessary to consult with specially trained personnel who have specific expertise in the types of digital devices, operating systems, or software applications that are being searched.

b. Digital data is particularly vulnerable to inadvertent or intentional modification or destruction. Searching digital devices can require the use of precise, scientific procedures

that are designed to maintain the integrity of digital data and to recover "hidden," erased, compressed, encrypted, or password-protected data. As a result, a controlled environment, such as a law enforcement laboratory or similar facility, is essential to conducting a complete and accurate analysis of data stored on digital devices.

c. The volume of data stored on many digital devices will typically be so large that it will be highly impractical to search for data during the physical search of the premises. A single megabyte of storage space is the equivalent of 500 double-spaced pages of text. A single gigabyte of storage space, or 1,000 megabytes, is the equivalent of 500,000 double-spaced pages of text. Storage devices capable of storing 500 or more gigabytes are now commonplace. Consequently, just one device might contain the equivalent of 250 million pages of data, which, if printed out, would completely fill three 35′ x 35′ x 10′ rooms to the ceiling. Further, a 500 gigabyte drive could contain as many as approximately 450 full run movies or 450,000 songs.

d. Electronic files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted, or viewed via the Internet. Electronic files saved to a hard drive can be stored for years with little or no cost. Even when such files have been deleted, they can be recovered months or years later using readily-available forensics tools. Normally, when a person deletes a file on a computer, the data contained in the file does not

actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space, i.e., space on a hard drive that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space, for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a swap or recovery file. Similarly, files that have been viewed on the Internet are often automatically downloaded into a temporary directory or cache. The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently downloaded or viewed content. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer habits. Recovery of residue of electronic files from a hard drive requires specialized tools and a controlled laboratory environment. Recovery also can require substantial time.

e. Although some of the records called for by this warrant might be found in the form of user-generated documents (such as word processing, picture, and movie files), digital devices can contain other forms of electronic evidence as well. In particular, records of how a digital device has been used, what it has been used for, who has used it, and who has been responsible for creating or maintaining records, documents,

programs, applications and materials contained on the digital devices are, as described further in the attachments, called for by this warrant. Those records will not always be found in digital data that is neatly searchable from the hard drive image as a whole. Digital data on the hard drive not currently associated with any file can provide evidence of a file that was once on the hard drive but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave digital data on the hard drive that show what tasks and processes on the computer were recently used. Web browsers, e-mail programs, and chat programs often store configuration data on the hard drive that can reveal information such as online nicknames and passwords. Operating systems can record additional data, such as the attachment of peripherals, the attachment of USB flash storage devices, and the times the computer was in use. Computer file systems can record data about the dates files were created and the sequence in which they were created. This data can be evidence of a crime, indicate the identity of the user of the digital device, or point toward the existence of evidence in other locations. Recovery of this data requires specialized tools and a controlled laboratory environment, and also can require substantial time.

f. Further, evidence of how a digital device has been used, what it has been used for, and who has used it, may be the absence of particular data on a digital device. For example, to

rebut a claim that the owner of a digital device was not responsible for a particular use because the device was being controlled remotely by malicious software, it may be necessary to show that malicious software that allows someone else to control the digital device remotely is not present on the digital device. Evidence of the absence of particular data on a digital device is not searchable from the digital device. Analysis of the digital device as a whole to demonstrate the absence of particular data requires specialized tools and a controlled laboratory environment, and can require substantial time.

13. Other than what has been described herein, to my knowledge, the United States has not attempted to obtain this data by other means.

VII. CONCLUSION

14. For all the reasons described above, there is probable cause to believe that evidence of violations of the **Target Offenses**, as described above and in Attachment B of this affidavit, will be found in searches of the **Target Locations**, as further described above and in Attachment A of this affidavit.

/S/

William Cone III, Special Agent, Federal Bureau of Investigation

Subscribed to and sworn before me this 8 day of September, 2015.

Suzanne H. Segal

HONORABLE SUZANNE H. SEGAL
UNITED STATES MAGISTRATE JUDGE